

Geavanceerde instellingen voor site-to-site VPN en failover op de RV160 en RV260

Doel

Het doel van dit document is u te tonen hoe u de site-to-site VPN geavanceerde instellingen en failover op de RV160 en RV260 kunt configureren.

Inleiding

Een Virtual Private Network (VPN) is een goede manier om externe medewerkers aan te sluiten op een beveiligd netwerk. Een VPN kan een externe host inschakelen om op te treden alsof ze was verbonden met het beveiligde on-site netwerk. In een site-to-site VPN sluit de lokale router op één locatie zich aan op een externe router door een VPN-tunnel. Deze tunnel kapselt gegevens veilig in door middel van industriestandaard encryptie- en authenticatietechnieken om verzonden gegevens te beveiligen. Aan beide zijden van de verbinding moet een identieke configuratie worden uitgevoerd, zodat een succesvolle site-to-site VPN-verbinding kan worden gerealiseerd. Geavanceerde site-to-site VPN-configuratie biedt de flexibiliteit om optionele configuraties te configureren voor de VPN-tunnel.

Failover is een krachtige optie die een constante verbinding tussen deze twee sites garandeert. Dit is handig wanneer fouttolerantie belangrijk is. Een failover komt voor wanneer de primaire router neer is. Op dit punt zal een secundaire of backup router de projector overnemen en een verbinding leveren. Dit helpt een enkel punt van falen te voorkomen.

Toepasselijke apparaten

RV160

RV260

Softwareversie

•1.0.00.13

Voorwaarden

Alvorens geavanceerde instellingen en failover voor site-to-site VPN op RV160 en RV260 te configureren moet u IPsec-profiel en site-to-site VPN op uw lokale en externe router configureren. Hieronder staat een lijst met artikelen die u kunnen helpen bij de configuratie ervan. U kunt de optie gebruiken om de VPN-wizard te gebruiken die u helpt bij de configuratie van zowel IPsec-profiel als site-to-site VPN. U kunt de wizard afzonderlijk configureren en volgen op de twee documenten die hieronder worden meegeleverd.

1. [VPN-setup-wizard configureren op de RV160 en RV260](#)

Of

1. [IPSec-profielen configureren \(Auto Keying Mode\) op de RV160 en RV260](#) (optioneel)
2. [Site-to-site VPN configureren op de RV160 en RV260](#)

Geavanceerde instellingen voor site-to-site VPN

De geavanceerde instellingen moeten aan beide zijden van de VPN-verbinding hetzelfde worden ingesteld.

Stap 1. Meld u aan bij het programma voor webconfiguratie.



Router

cisco

●●●●●●●●

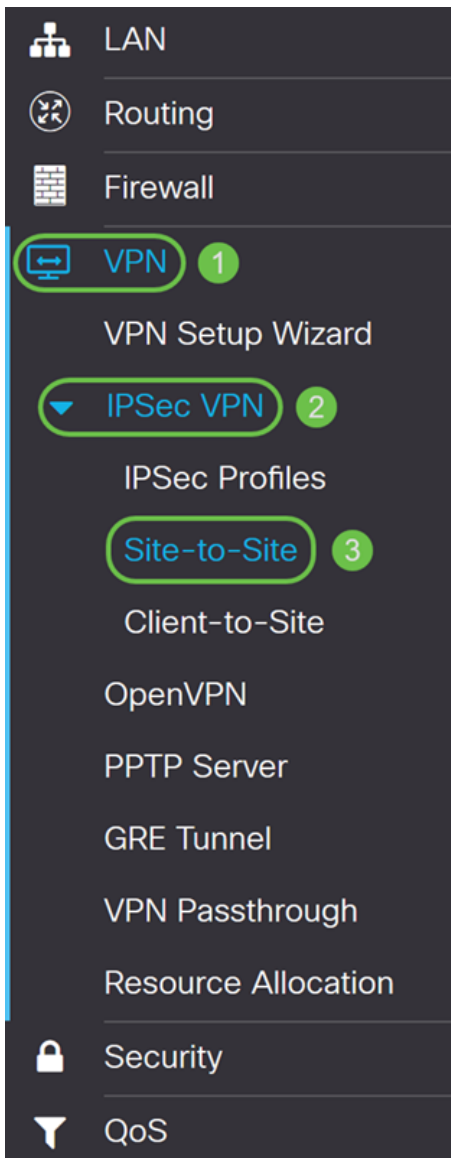
English ▼

Login

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.




Stap 2. Navigeer naar **VPN > IPSec VPN > Site-to-Site**.




Stap 3. Controleer het vakje voor de verbinding die u wilt bewerken. Druk vervolgens op het pictogram **pen en papier** om de verbinding te bewerken. In dit voorbeeld wordt de verbinding genaamd HomeOffice geselecteerd.

Site-to-Site Apply Cancel

Number of Connections: 1 connected, 1 configured, maximum 10 supported.

2   

<input type="checkbox"/>	Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions
1 <input checked="" type="checkbox"/>	HomeOffice	140. [redacted]	WAN	VPNTest	10.1.1.0/24	192.168.2.0/24	Connected	

Stap 4. Klik op het tabblad **Geavanceerde instellingen**.

Add/Edit a New Connection Apply Cancel

Basic Settings **Advanced Settings** Failover

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Stap 5. Controleer het vakje **Compress (Support IP payload Compression Protocol (IPComp))** om de router in staat te stellen om compressie voor te stellen wanneer deze een verbinding start. Dit protocol beperkt de omvang van IP-datagrammen. Als de responder dit voorstel afwijst, dan voert de router geen compressie uit. Wanneer de router de responder is, accepteert het compressie, zelfs als compressie niet ingeschakeld is. Als u deze eigenschap voor deze router toelaat, zou u het op de verre router (het andere eind van de tunnel) moeten toelaten.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Stap 6. Broadcast-berichten worden gebruikt voor naamresolutie in Windows-netwerken om bronnen zoals computers, printers en bestandsservers te identificeren. Deze berichten worden gebruikt door bepaalde softwaretoepassingen en Windows-functies, zoals de netwerkbuurt. LAN-uitzendverkeer wordt normaal niet via een VPN-tunnel doorgestuurd. U kunt dit vakje echter aanvinken om de NetConfiguration-uitzendingen vanuit het ene uiteinde van de tunnel naar het andere uiteinde te kunnen doorsturen. Controleer het selectieknop **NetVIB Broadcast** om dit mogelijk te maken.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Stap 7. Controleer het selectieteken **Houd-bewegend** toetsenbord om de router in staat te stellen de VPN-verbinding opnieuw op te bouwen met regelmatige tussenpozen van de tijd. Voer het aantal seconden in om het *Houd-levendige* controleinterval in het veld *Controle* van *het Onderhouden* in te stellen. De marge is van 10-999 seconden.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive **1** **2**

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Stap 8. Controleer **Dead Peer Detection (DPD)** ingeschakeld om DPD in te schakelen. Het stuurt periodieke HELLO/ACK-berichten naar de status van de VPN-tunnel. De DPD optie moet aan beide uiteinden van de VPN-tunnel zijn ingeschakeld. Specificeer het interval tussen HELLO/ACK berichten in het veld Interval door het volgende in te voeren:

Vertraging - Voer de vertraging in seconden in tussen elk Hallo bericht. Het bereik loopt van 10 tot 300 seconden en de standaardwaarde is 10.

Time-out bij detectie - Voer de tijd in seconden in om te verklaren dat de peer dood is. Het bereik loopt van 30 tot 1800 seconden.

DPD Actie - Actie te nemen na de DPD-onderbreking. Selecteer in de vervolgkeuzelijst **Verwijderen** of opnieuw **starten**.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled **1**

Delay Time: **2** sec. (Range: 10 - 300)

Detection Timeout: **3** sec. (Range: 30 - 1800)

DPD Action: **4**

Extended Authentication

User

User Name

Stap 9. Controleer **Uitgebreide verificatie** als u uitgebreide verificatie wilt inschakelen. Dit zal een extra niveau van authenticatie opleveren dat van externe gebruikers vereist is om in hun geloofsbrieven te toetsen voordat ze toegang tot VPN krijgen. Om uitgebreide authenticatie te krijgen om te kunnen werken moet de hoofdsite groepsidentificatie gebruiken en de externe site moet gebruikmaken van gebruikersverificatie. In de volgende paar stappen zullen we de hoofdsite configureren om groepsverificatie te gebruiken.

Opmerking: Aanbevolen wordt om client-to-Site te configureren voor gebruikersverificatie in plaats van uitgebreide verificatie.

Als u nog geen gebruikersgroep voor uw hoofdsite hebt gemaakt, klikt u op de link om te leren hoe u een gebruikersgroep in dit artikel kunt maken: [Een gebruikersgroep maken voor uitgebreide verificatie](#).

Als u wilt leren hoe u gebruikersaccounts kunt maken, klikt u op de link die naar de sectie wordt teruggestuurd: [Een gebruikersaccount maken voor uitgebreide verificatie](#).

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

Group:



Group Name

Stap 10. Selecteer **Groep** als de uitgebreide verificatie en druk op het **plus**-pictogram om een nieuwe groep toe te voegen. Kies in de vervolgkeuzelijst de groep die u voor de verificatie wilt gebruiken. Zorg ervoor dat de gebruikers die u wilt in die groep zitten.

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

1 Group: **2**

Group Name

3

Stap 1. In de volgende paar stappen zullen we de afstandsrouter configureren om gebruikersverificatie te gebruiken. In de router op afstand controleert u het vakje **Extended Verificatie** om uitgebreide verificatie mogelijk te maken.

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

Group:

Group Name

Stap 12. Selecteer **Gebruiker** als uitgebreide verificatie. Voer de **gebruikersnaam** en het **wachtwoord** in van de gebruiker in de groep die in de hoofdrouter is geselecteerd. In dit voorbeeld, VPNuser en CiscoTest123! werd ingevoerd.

Extended Authentication

1 User

User Name

2 VPNUser

Password

3

Show Password:

Enable

Group:



Group Name

Stap 13. Controleer **DNS-splitter** om dit mogelijk te maken. Hiermee worden de Domain Name System (DNS)-server en andere DNS-verzoeken op een andere DNS-server verdeeld, op basis van gespecificeerde domeinnamen. Wanneer de router een verzoek om adresresolutie ontvangt, inspecteert het de domeinnaam. Als de domeinnaam overeenkomt met een domeinnaam in de DNS-instellingen splitsen, wordt het verzoek doorgegeven aan de gespecificeerde DNS-server in het VPN-servernetwerk. Anders wordt het verzoek doorgegeven naar de DNS-server die wordt gespecificeerd in de WAN-interfaceinstellingen (d.w.z. de DNS-server van de ISP).

Split DNS wordt voor hetzelfde domein in twee zones gescheiden. Het ene wordt gebruikt door het interne netwerk en het andere door het externe netwerk. Splitst DNS richt interne hosts op een interne DNS voor naamresolutie en externe hosts worden gericht op een externe DNS voor naamresolutie.

Als u *DNS-splitter* hebt ingeschakeld, geeft u het IP-adres van de DNS-server in om voor de gespecificeerde domeinen te gebruiken. Specificeer optioneel een secundaire DNS-server in het veld *DNS-server 2*. Voer in de *Domain Name 1-6* de domeinnamen in voor de DNS-servers. De verzoeken om de domeinen worden doorgegeven aan de gespecificeerde DNS server.

Split DNS 1

DNS Server 1:

2 192.168.1.80

DNS Server 2:

(Optional)

Domain Name 1:

3 www.cisco.com

Domain Name 2:

(Optional)

Domain Name 3:

(Optional)

Domain Name 4:

(Optional)

Domain Name 5:

(Optional)

Domain Name 6:

(Optional)

Stap 14. Klik op **Toepassen**.

Add/Edit a New Connection

Apply

Cancel

Group Name

Split DNS

DNS Server 1:

DNS Server 2: (Optional)

Domain Name 1:

Domain Name 2: (Optional)

Domain Name 3: (Optional)

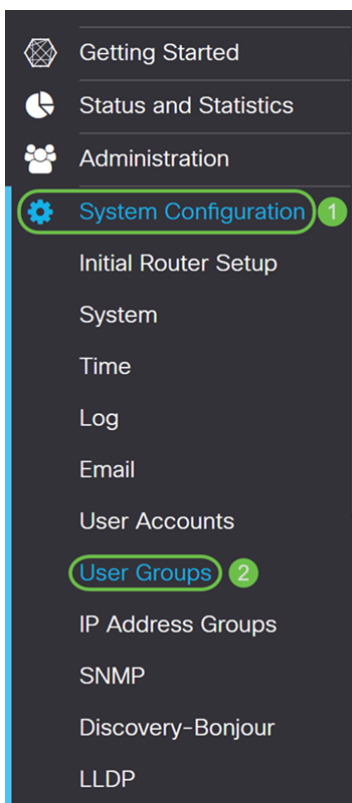
Domain Name 4: (Optional)

Domain Name 5: (Optional)

Domain Name 6: (Optional)

[Gebruikersgroep maken voor uitgebreide verificatie](#)

Stap 1. Navigeer naar **stelselconfiguratie** > **gebruikersgroepen**.



Stap 2. Klik op het pictogram **plus** om een nieuwe gebruikersgroep toe te voegen.

User Groups

Apply

Cancel



<input type="checkbox"/>	Group	Web Login /NETCONF /RESTCONF	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP
<input type="checkbox"/>	admin	Admin	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	guest	Disable	Disable	Disable	Disable	Disable	Disable

Stap 3. Voer een naam in het veld *groepsnaam in* en druk vervolgens op **Toepassen**. In dit voorbeeld werd SiteGroupTest ingevoerd als de groepsnaam.

User Groups

2

Apply

Cancel

Group Name:

1

Local User Membership List



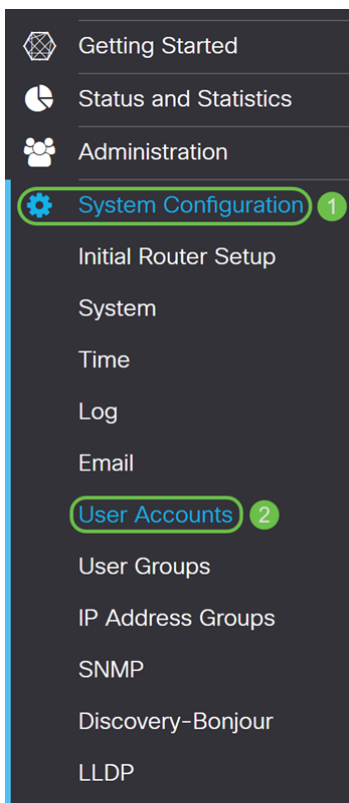
User

* Should have at least one account in the 'admin' group.

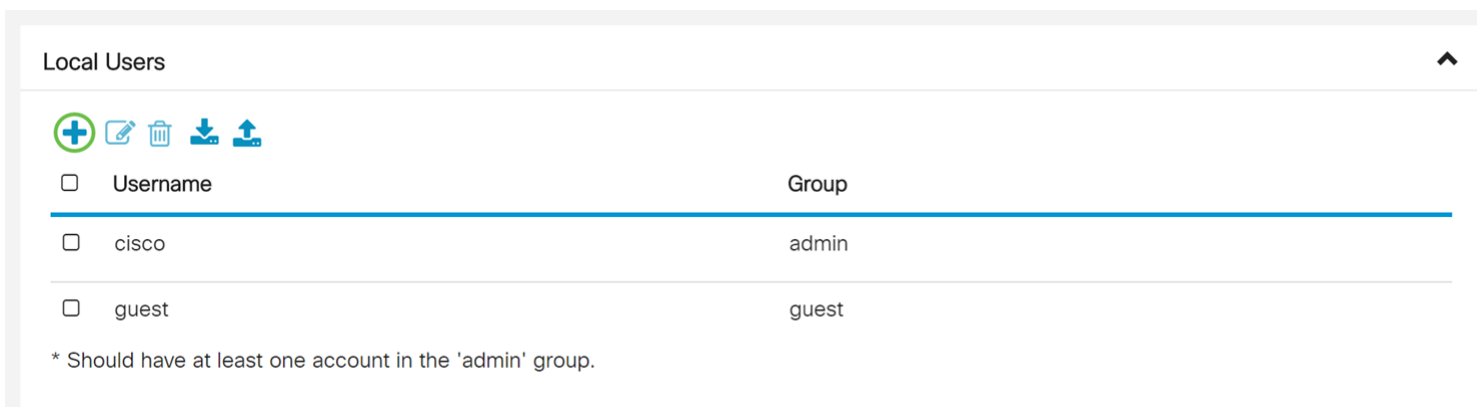
[Gebruikersrekeningen voor uitgebreide verificatie configureren](#)

Belangrijke opmerking: Laat de standaard-beheeraccount in de beheergroep achter en maak een nieuwe gebruikersaccount en gebruikersgroep voor Shrew Soft. Als u uw Admin-account naar een andere groep verplaatst, voorkomt u dat u zich in de router registreert.

Stap 1. Navigeer naar **stelsysteemconfiguratie > Gebruikersrekeningen**.




Stap 2. Scrollt door de pagina naar *lokale gebruikers*. Klik op het pictogram **plus** om een nieuwe lokale gebruiker toe te voegen.



Stap 3. De pagina *gebruikersaccount toevoegen* wordt geopend. Voer een gebruikersnaam in in het veld *Gebruikersnaam*. In dit voorbeeld werd VPN-gebruiker ingevoerd als de gebruikersnaam.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

Confirm Password:

Password Strength meter:

Group:

 ▼


Apply

Cancel

Stap 4. Voer een wachtwoord in in het veld *Nieuw wachtwoord* en *Wachtwoord bevestigen*. In dit voorbeeld, CiscoTest123! werd ingevoerd.

Opmerking: Dit wachtwoord is als voorbeeld gebruikt, maar er wordt een complexer wachtwoord aanbevolen.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

1

Confirm Password:

2

Password Strength meter:




Group:

Apply

Cancel

Stap 5. Selecteer een groep en druk vervolgens op **Toepassen** om uw nieuwe gebruikersaccount te maken. In dit voorbeeld werd SiteGroupTest als groep geselecteerd.

Add user account


 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

Confirm Password:

Password Strength meter: 

Group: 1

2

failover configureren

Om de site-to-Site failover mogelijk te maken, moet het inhoudprogramma ingeschakeld zijn op het tabblad *Geavanceerde instellingen*.

Stap 1. Klik op het tabblad **Failover** om de failover te configureren.

Add/Edit a New Connection

Basic Settings | Advanced Settings | **Failover**

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address)

Local Interface:

Stap 2. Controleer **Tunnel back-up** om deze te activeren. Wanneer de primaire tunnel onder is, stelt deze eigenschap de router in om de VPN-tunnel opnieuw in te stellen door of een afwisselend IP adres voor de afstandsbediening te gebruiken of een afwisselend lokaal WAN. Deze optie is alleen beschikbaar als DPD is ingeschakeld.

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address)

Local Interface:

Stap 3. In het veld *Remote Backup IP-adres* voert u het IP-adres in voor de externe peer, of geeft u het WAN IP-adres weer dat al voor de externe gateway is ingesteld. Selecteer vervolgens de lokale interface (**WAN1**, **WAN2**, **USB1** of **USB2**) in de vervolgkeuzelijst.

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address) **1**

Local Interface: **2**

Stap 4. Klik op **Toepassen**.

The screenshot shows the 'Add/Edit a New Connection' window with the 'Failover' tab selected. The 'Tunnel Backup' checkbox is checked. The 'Remote Backup IP Address' field contains '145.' followed by a redacted IP address. The 'Local Interface' dropdown menu is set to 'WAN'. There are 'Apply' and 'Cancel' buttons at the top right.

Conclusie

U moet nu met succes geavanceerde instellingen en failover voor uw site-to-site VPN op RV160 en RV260 hebben geconfigureerd. Uw site-to-site VPN moet nog verbonden zijn.

Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)